

## **MMD - Gifts and Hospitality Full Audit**

### **Executive Summary - Extract from audit report**

Owned by Portsmouth City Council, MMD is a multi-million cargo handling operation employing over 170 staff, ranging from crane drivers, customer account handlers, warehouse and container operatives, quayside staff, health and safety officers to HR and facilities experts.

As a general rule the organisation does not believe that giving and receiving gifts is appropriate to the efficient conduct of its organisation. An audit review of MMD Gifts, Hospitality and Entertainment processes for the financial year 2017/18 has been conducted as part of the 2018/19 Audit Plan.

**Compliance with Policies, Laws and Regulations Assurance Level: No Assurance**

#### Policies and Procedures

Testing has identified that there is a Gifts, Hospitality and Entertainment Policy, a Code of Conduct and an Anti-Bribery Policy in place, all of which make reference to the company's expectations with regard to the acceptance of gifts and hospitality, and provides detailed instruction on how to register receipt of any gifts and hospitality. Discussions with the Senior Human Resources Advisor have established that the Gifts, Hospitality and Entertainment Policy and Anti-Bribery Policy were both last reviewed in June of this year, 2018. The policies are held on the intranet and are accessible for staff that have access to the company network. Staff who are unable to access the network can request copies from their line manager.

Testing sourced a copy of a new starter checklist which includes details of policies and documents that are to be shared with new starters. The three above mentioned policies are recorded on this list. New staff members are required to sign a Code of Conduct declaration which asks the employee to confirm that they have read and understood their obligations under section 11 of the policy - "Gifts, Hospitality and Entertainment". Testing reviewed 18/176 (10%) employee HR records and identified that 15/18 (83%) employees had signed the Code of Conduct declaration. Only 5/15 (33%) had received a signature from a Line Manager to confirm that new employees had been made aware of these policies.

#### Acceptance, Rejection and Recording of Gifts and Hospitality

Testing has established that there is no evidence that there is a gifts and hospitality register at MMD. Actions agreed as part of the MMD payroll audit of 2012/13 (PCC12/13-134) confirmed that a gifts and hospitality register had been introduced and was in use as

## Appendix B - Areas of concern & update on previous No Assurance Audits

at December 2012. However, an email to Internal Audit from the Financial Controller and Senior HR Advisor on 3<sup>rd</sup> October 2018 confirms that there is no register in place.

In the absence of a Gifts and Hospitality Register staff and stake holders are unable to identify who donated and received gifts or hospitality. In addition, it has not been possible to evidence that there are any mechanisms in place to monitor the giving or receiving of gifts or hospitality, or if any non-compliance has been handled appropriately.

### **Completion of the audit Assurance Level: No Assurance**

In summary, while it is noted that company policies do include reference to gifts and hospitality, a no assurance opinion has been given as there is no mechanism in place to record or monitor the offering/acceptance and rejection of gifts and hospitality, or address any non-compliance with regard to MMD's Policies. Therefore, Internal Audit is unable to test and quantify the levels of gifts and hospitality that have been received and declared. As such it is not possible to provide any assurance that this area is of low risk to the company due to the potential financial, reputational and legislative risks that may arise from a lack of transparency in this area.

Whilst, the giving of gifts and hospitality are common practice in conducting business, there are some occasions where such practices are perceived as inappropriate or potentially fraudulent. Internal Audit has, over the years, investigated numerous allegations of bribery against MMD staff which have been communicated to either previous or existing board members. The risks surrounding this area relate to fraud, bribery & corruption; therefore robust controls should be in place to safeguard both individuals and the company.

## **MMD - Procurement - Follow Up**

### **Executive Summary - Extract from audit report**

An audit of the procurement process at MMD was undertaken during 2017/18. The issues raised, and actions agreed, have been followed-up and reported below, in accordance with the 2018/19 Audit Plan.

**Previous Compliance with Policies, Laws and Regulations Assurance Level: No Assurance**  
**Current Compliance with Policies, Laws and Regulations Assurance Level: Limited Assurance**

### **Procurement Framework**

#### *Original Testing*

A concern was raised in the 2017/18 audit as it was not possible to establish details of any quote or tendering process. It was not possible to obtain documentation to show at what level staff could seek quotes, how many comparative quotes should be sought from suppliers, how suppliers should be sourced, and at what financial level contracts should be put out to tender. There was no review of supplier performance by way of a formalised Key Performance Indicator process.

#### *Follow-Up Testing*

Follow-up enquiries revealed that a procurement policy has been formulated, including information about the purchasing authority thresholds and a requirement to seek comparative quotes for procurements over £30k. There is reference to the requirement to keep all documentation involved in a tender exercise, but no details regarding in what circumstances one should be undertaken. The policy is specific that all information relevant to suppliers and procurements should be stored within the new database, 'My Compliance'.

The policy is not explicit as to how suppliers should be sourced, or how contracts should be monitored; however there is a requirement that records and data systems are maintained in such a way as to provide an appropriate, auditable, trail of each purchasing activity, including the ability to monitor supplier performance.

## Appendix B - Areas of concern & update on previous No Assurance Audits

The policy makes specific reference that a desired outcome is that of greatest value gained at the lowest total cost; however, as all 26 of the new suppliers tested fell below the £30k threshold at which quotations are required, it has not been possible to evidence how this aim is being achieved.

### Supplier Contracts and Set-Up

#### *Original Testing*

A concern was raised as part of the 2017/18 audit, as testing was unable to source contracts or supplier set-up forms for a number of suppliers within a sample. The audit also raised concerns that where supplier set-up forms were present, they were not clearly authorised, and not all gave consideration to the annual or lifetime cost of the service.

#### *Follow-Up Testing*

Queries with the MMD Financial Controller revealed that there have been 26 new suppliers added to the system since the previous audit was completed in May 2018. Testing sought to establish that the procurements had been made in accordance with the new procurement policy, and that records were being held within the 'My Compliance' database as advised within the previous report.

Interrogation of the 'My Compliance' database revealed that 16/26 (62%) suppliers appeared to have been set up in accordance with the new policy. These entries contained appropriately authorised supplier set-up forms, with a clear annual cost. All were for single payments, rather than ongoing contracts. A further 1/26 (4%) was found not to be relevant, as it related to an employee that had been set up as a means to receive expenses. Of the remaining nine:

- 1/9 (11%) supplier could not be located within the database.
- 3/9 (33%) related to recruitment contracts; however, the signed contract terms had not been uploaded to the database.
- 5/9 (56%) had supplier set-up forms that did not contain the anticipated annual cost. It was not possible to establish this cost from the associated documentation.

After clarification with the MMD Financial Controller:

- The missing supplier was added to the database and was seen to have been compliant with the proposed procurement policy.

## Appendix B - Areas of concern & update on previous No Assurance Audits

- All three terms of business for the recruitment contracts were added to the database.
- Documents had been added to show the anticipated annual cost for 3/5 of the suppliers missing those details; however, these quotes were shown in an email, sent subsequent to the authorisation of the set-up form.
- The remaining two suppliers had documentation uploaded to indicate either rates, or costs for a proposed single order, but did not indicate what the potential annual cost would be. It is possible that this information could not have been known at the time that the authorisation was made, but without further documentation, it is not possible to confirm.

KPI monitoring was not found to be relevant to any of the new supplier procurements; however, the MMD Financial Controller provided details of a cleaning contract, which would have been subject to KPI monitoring. It was not possible to see a copy of the contract within the My Compliance file; however, there was evidence to indicate that monitoring had been undertaken on the quality of the service in April and June 2018.

**Previous Effectiveness & Efficiency of Operations Assurance Level: Assurance**

**Current Effectiveness & Efficiency of Operations Assurance Level: Assurance**

No further testing has been undertaken under this header.

**Previous Completion of the audit Assurance Level: No Assurance**

**Current Completion of the audit Assurance Level: Limited Assurance**

Two high-risk exceptions, relating to the procurement framework and supplier set-up, remain in progress after the completion of audit testing. Although a procurement policy has been formulated, and there is a more structured approach to record keeping, concerns remain over the quotation threshold, and the ability to demonstrate transparent procurement and value for money for contracts under £30,000. Furthermore, though there appears to have been a significant improvement on both the quantity and quality of procurement records kept, there are still questions surrounding the authorisation of forms where the anticipated costs have not been known, and the ability to demonstrate that the appropriate type of procurement has been authorised. As a result, Internal Audit can provide limited assurance that the procurement process at MMD is of low risk to the business.

## **IT Procurement, Inventory and Disposal - Follow Up**

### **Executive Summary - Extract from audit report**

As part of the previous audit review, one critical and six high risk exceptions were raised. Overall, a no assurance opinion was reached as a result of inaccurate IT equipment inventory records, partially restricted access to new IT assets and those awaiting redeployment, and the absence of a contract with the company currently disposing of the Council's IT equipment. These weak internal controls could have potentially resulted in reputational, operational, legislative and financial risks to the authority.

Discussions with the Assistant Director of Contracts, Procurement and Commercial during the audit exit meeting in February 2018 confirmed that on-going works to improve the IT inventory process by introducing a new IT management system (ITSM) by April 2018, would mitigate the risks identified as a result of the previous audit. However, until the new IT management system is in place, Internal Audit could give no assurance on the effectiveness of the IT Procurement, Inventory and Disposal process.

A follow up audit has been conducted as part of the 2018/19 audit plan to review the progress of the agreed actions and the implementation of the new ITSM and processes.

**Previous Achievement of organisation's strategic objectives Assurance Level: Limited Assurance**

**Achievement of organisation's strategic objectives Assurance Level: Assurance**

One high risk exception was raised as a result of previous audit testing, as the departmental disposal and redeployment guidance had not received regular review and information contained within the documents was out of date. In addition, the Council's Financial Rules had not received a review within the last 12 months.

Follow up testing has identified that the Asset and Inventories section of the Financial Rules has been reviewed and the Deputy Director of Finance and S151 Officer has advised that no changes were to be made. Departmental Redeployment and Disposal Guidance has also received a review by IT and new procedures have been made accessible for all IT staff members. In addition, copies of an IT asset disposal and redeployment work process flow chart has been displayed in the IT warehouse as a reminder for IT staff when transferring assets. Discussions with the Information Security Officer have established that the Hardware and Keep IT

## Appendix B - Areas of concern & update on previous No Assurance Audits

Secure and Legal policies have also been reviewed to reflect the introduction of GDPR; however a timescale for publication could not be confirmed at the time of testing.

**Previous Compliance with Policies, Laws and Regulations Assurance Level: No Assurance**

**Compliance with Policies, Laws and Regulations Assurance Level: Limited Assurance**

Three high risk and one critical risk exceptions were raised as a result of previous audit testing with regards to the high value of unallocated assets, the inconsistency of information recorded on the inventory, the absence of a disposal authorisation process and disposal contract.

Follow up testing confirmed:

- The value of unallocated assets as at 31 August 2018 was £1229.08 and this figure relates to small value items not covered by financial rule L5 such as cables and port adapters. (1.9% of the total value of assets not yet recharged to customers - £64454.56)
- A review of inventory records for 10/53 randomly selected laptops purchased in 2018, identified 9/10 records were completed in accordance with section L5 of PCCs Financial Rules. 1/10 of the records was showing as "in use" but the location of the item was recorded as being in the warehouse.
- There is currently a temporary process in place in which the Operations Manager reviews and authorises requests to dispose of inadequate IT equipment. This process will be replaced by line management authorisation when a new self-serve customer portal is operational in vFire, the new ITSM.
- As of 6 June 2018 there is a new IT waste disposal contract and tracking process in place to collect and dispose or recycle IT equipment.

**Previous Safeguarding of Assets Assurance Level: Limited Assurance**

**Safeguarding of Assets Assurance Level: Limited Assurance**

Two high risk exceptions had been raised as a result of previous audit testing with regard to incorrect inventory records, and equipment not being security marked.

## Appendix B - Areas of concern & update on previous No Assurance Audits

Follow up review has established that the data transfer from Eworks to vFire is now complete. Discussions with the Operations Manager have identified that Helpdesk Operatives are updating User and Net ID as and when equipment comes into contact with the IT Helpdesk. In addition, a Windows 10 asset audit had identified equipment in use throughout PCC, and this information will be entered into vFire by the end of October 2018 to update records ready for the Windows 10 software rollout.

A review of the new warehouse "BIN" storage and naming system has highlighted improvements in the storage of new and redeployed stock. Inventory records now detail the location of assets by identifying a shelf number and shelf position. Testing selected a random sample of 20/195 items listed on the inventory as being located in the warehouse, and compared inventory records with the actual location of the asset. The location of 18/20 items were recorded accurately on the inventory. 2/20 items were later found to be in use, however the inventory had not been updated to reflect this. Testing also selected 10 items from the shelf and compared their location with that recorded on the inventory, and confirmed that 100% of these items were recorded accurately.

Discussions with the Operations Manager have established that the IT Team are working towards assigning a net ID number and a QR code to new high value stock so that an operative can instantly locate an asset's record on vFire by scanning the QR code. This project is to be completed and in use by the end of January 2019.

The possibility of having security etchings added to high value items was explored; however the cost per item for this security measure is £6. It has agreed by the service that etching was not cost effective and having the serial number recorded on vFire would ensure the asset was traceable.

**Previous Effectiveness & Efficiency of Operations Assurance Level: Limited Assurance**

**Effectiveness & Efficiency of Operations Assurance Level: Limited Assurance**

Previous testing identified that there were no processes in place to record the transfer of assets from "in use" status to "redeployed". Follow up discussions with the Operations Manager have established that vFire will be used to record the full history of an IT asset. Each time the asset comes into contact with the IT Service, a record will be made on vFire, and the status of the item will also be updated. This has not been verified by Internal Audit as the vFire inventory is not yet complete. All external sources of inventory information will be fed into vFire before the end of October 2018. Further detail can be found in exception ISS.6 in the main body of the report.



Appendix B - Areas of concern & update on previous No Assurance Audits

**Previous Completion of the audit Assurance Level: No Assurance**

**Completion of the audit Assurance Level: Limited Assurance**

Five high risk exceptions remain in progress as a result of follow up testing, as the new ITSM due to go live in April 2018 was not in use until September 2018, and although significant progress has been made, many of the processes are still in their infancy within the IT department and not yet embedded corporately.